REMARKS

This Response is in response to the Office Action dated April 9, 2003. Claims 1-39 are pending, and claims 1, 6, 24, and 29 have been amended. Consequently, claims 1-39 remain pending.

In the Drawings, FIG. 7A has been amended to replace the word "Hose" with "Host." A corrected drawing showing the changes in red is attached. In the Specification, the serial number, title, and filing date of a pending application has been provided. Claims 1 and 24 have been amended to correct typographical errors. Claims 6 and 29 have been amended to recite a "dynamic key", rather than a "key" to provide proper antecedent basis. Accordingly, no new matter has been entered.

Attorney for applicant acknowledges and appreciates the telephone interview with the Examiner on June 4, 2003, the substance of which is discussed below.

The Examiner rejected claims 1-39 under 35 USC §102(b) as being anticipated by Chou et al. (US Pat. No. 5,222,133). Applicant respectfully traverses the rejection.

The present invention provides a method for protecting software from unauthorized use. The present invention works in cooperation with a portable external security device that plugs into the computer system on which encrypted software is to be run. Referring to FIG. 8, at least two hidden keys are used key to create additional keys for encrypting/decrypting the software, initialization vector 711 and the dynamic key 712. According to the present invention, the initialization vector 711 is bundled with the encrypted software in authorization program 801, which is run on the computer system, and the dynamic key 712 is stored in the security device 131 to protect the hidden keys from discovery. When a user attempts to use the protected software on the computer system, the initialization vector 711 is passed from the computer system to the security device; and the security device uses the two hidden keys to generate an

encryption key, shown as security key 714. The security device then transfers the security key to the computer system, where it is used to decrypt and execute the encrypted software. These steps are particularly recited in the independent claims, such as claim 16, for example.

According to the present invention, the protected software only contains part of the information needed for decryption, and must receive the remaining information from the security device before the software can be used. Similarly, the security device can't generate the encryption key without receiving information from the software.

In a further aspect of the present invention, the security device scrambles the encryption key prior to transferring it to the software, thus providing a secure transaction between the security device and the software. The software must contain addition information to descramble the encryption key before the encryption key can be used to decrypt the software. The additional information is temporary, and is forgotten once the protected software is enabled. Thus, for each invocation of the protected software, the appropriate secure transaction must take place successfully.

In contrast to the present invention, Chou teaches storing a first key in a plug-in security device, and during software authorization on the computer, the key is retrieved from the security device. A user of the computer then enters a second key, and the software on the computer uses the first and second keys to generate a control key, which is then used to authorize the software.

Chou fails to teach or suggest the claims of the present invention, such as claim 1, for several reasons. First, step (b) of claim recites "authorizing use of the software on the computer system by generating the encryption key *within the security device using information supplied from the software*." Chou, in contrast, teaches that the control key is generated on the computer, rather than in the security device. In addition, because the control key is generated on the computer, Chou teaches that the first key is passed from the security device to the computer. Step (b) of claim

1, however, recites that the encryption key is generated "using information supplied from the software," which in the preferred embodiment is the initialization vector. Thus, Chou teaches the opposite of step (b). Instead of passing information from the computer to the security device to generate the encryption key on the security device, Chou teaches passing information from the security device to the computer to generate the control key on the computer.

Second, step (c) of claim 1 recites "sending the encryption key from the security device to the computer system for decryption of the software." As stated above, Chou creates the control key on the computer system where the software is authorized. Therefore, step (c) is wholly missing from the teaching of Chou.

Therefore, for the above identified reasons, the present invention as recited in independent claims 1-39 is neither taught nor suggested by Chou. In view of the foregoing, Applicant submits that claims 1-39 are patentable over the cited reference. Applicant, therefore, respectfully requests reconsideration and allowance of the claims as now presented.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,

June 30, 2003
Date

Stephen Sullivan
Sawyer Law Group LLP
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540